REMARKS

In the Final Office Action, Examiner Nguyen rejected pending claims 9-40 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,146,498 to *Smith*. The Applicant has thoroughly considered Examiner Nguyen's remarks concerning the patentability of pending claims 9-40 over *Smith*. The Applicant has also thoroughly re-read *Smith*. The Applicant respectfully asserts that Examiner Nguyen still does not have a proper understanding of *Smith*. Again, the Applicant therefore provides the following explanation of FIGS. 1 and 2 of *Smith* to facilitate a proper understanding of *Smith* by Examiner Nguyen.

As illustrated in FIGS. 1 and 2, *Smith* teaches a method for changing a key by a subscriber unit 10 and a method for generating a change key command by a central controller 20, respectively. In operation, whenever subscriber unit 10 needs to be rekeyed as determined in a step 14 (FIG. 2), central controller 20 sends a key change command with op code to subscriber unit 10 as shown in a step 21 (FIG. 2). Upon receipt of the key change command in a step 2 (FIG. 1), subscriber unit 10 decodes the op code in a step 24 (FIG. 1) to thereby generate a new key in step 26 (FIG. 1) and sends an acknowledge tone that the new key has been generated in a step 28 (FIG. 1).

Upon receipt of the acknowledge tone in a step 32 (FIG. 2), central controller 20 returns to step 14 (FIG. 2) to await a determination that a radio needs to be rekeyed. Conversely, upon a failure to receive the acknowledge tone in step 32 (FIG. 2), central controller 20 proceeds to a step 34 (FIG. 2) to determine whether to resend the key change command with op code in step 21 (FIG. 2) or to place subscriber unit 10 on a list of radios that need rekeying in a step 36 (FIG. 2). Central controller 20 may loop through steps 21, 32 and 34 before proceeding to step 36. See, *Smith* at column 2, line 66 to column 4, line 8.

One issue related to an interpretation of *Smith* is whether subscriber unit 10 encodes the acknowledge tone with the new key in step 28 (FIG. 1). Explicitly, *Smith* is silent as to whether the acknowledge tone is or is not encoded. Implicitly, *Smith* indicates the acknowledge tone IS NOT encoded by failing in step 21, step 32, step 34 and/or an additional step to teach (1) an attempt to decode the acknowledge tone with the new key by central controller 20 to thereby determine whether the acknowledge tone was properly encoded by subscriber unit 10 with the new key, (2) upon decoding the encoded acknowledge tone with the new key, a transmission of a signal from central controller 20 to subscriber unit 10 that verifies the decoding of the encoded acknowledge tone with the new key by central controller 20, and (3) upon failing to decode the encoded acknowledge tone with the new key, a transmission of a signal from central controller 20 to subscriber unit 10 that communicates the failure by central controller 20 to decoding the encoded acknowledge tone with the new key.

Specifically, an encoding of the acknowledge tone with the new key by subscriber unit 10 merits an attempted decoding of the encoded acknowledge tone central controller 20 upon receiving the encoded acknowledge tone. This attempted decoding further merits a determination by central controller 20 as to whether the acknowledge tone was properly encoded with the new key. Logically, a failure by *Smith* to teach a determination by central controller 20 as to whether the acknowledge tone was properly encoded with the new key unequivocally indicates an intention by Smith NOT to encode the acknowledge tone with the new key, old key or any other key.

By comparison, as illustrated in FIG. 5 for example, the present application discloses a cipher key change involving a transmission of a cipher change command CCC2 (coded with the old cipher key) from a radio network controller ("RNC") to a terminal ("TM"). After terminal TM has received cipher change command CCC2, an acknowledge command ACK12 is transmitted to radio network controller RNC to thereby prevent radio network controller RNC from retransmitting the cipher change command CCC2 after a specific period of time. Terminal TM thereafter transmits a cipher key acknowledge command CCOK2 (coded with the new cipher key) to radio

network controller RNC, which announces the reception of the cipher key acknowledge command CCOK2 by radio network controller RNC by means of an acknowledge command ACK22. Radio network controller RNC attempts to decipher cipher key acknowledge command CCOK2 with the new cipher key to determine whether cipher key acknowledge command CCOK2 was properly encoded with the new key by terminal TM. If acknowledge command CCOK2 was properly encoded with the new key by terminal TM, then radio network controller RNC transmits a match command KOK2 coded with the new cipher key to terminal TM to indicate a successful key change. Otherwise, radio network controller RNC transmits match command KOK2 coded with the old cipher key to terminal TM to indicate an unsuccessful key change. See, *U.S. Patent Application Serial No. 09/718,247* at page 6, line 16 to page 8, line 17.

Unequivocally, a proper understanding of *Smith* reveals that *Smith* does not teach or suggest any signal comparable to coded cipher key acknowledge command CCOK2 and coded match key command KOK2 as taught by the present application.

Moreover, *Smith* teaches away from a coding of the acknowledgement of step 28 (FIG. 1). Specifically, one benefit of the key change method of *Smith* is an elimination of a prior art need to use a data channel as the channel for implementing exchanging key information between subscriber unit 10 and central controller 20. See, *Smith* at column 1, line 46 to column 2, line 12; and column 5, line 61 to column 6, line 2. The benefit entails the efficient use of a control channel by central controller 20 to simultaneously send the digital word 42 (FIG. 3) to a plurality of subscriber units 10 without consuming a lot of air time and any additional system access time over the control channel.

Smith further teaches that any new key resulting from digital word 42 is to be used to encrypt and decrypt data/voice over the data channel. See, *Smith* at column 1, line 46 to column 2, line 12; and column 5, line 61 to column 6, line 2. *Smith* neither teaches nor ever intended the new key to be used to encrypt and decrypt control information (e.g., an acknowledgment tone) over the control channel. This is supported by the fact that such encryption and decryption of control information from a plurality of subscriber units 10 would consume additional air time and require additional system access time, which is in direct contradiction to the objectives of *Smith*.

Examiner Nguyen's Remarks. In the Final Office Action, Examiner Nguyen respectfully asserts that the Applicant erroneously asserts that *Smith* does not teach a key change command including a new cipher key. However, while the Applicant has correctly asserted that *Smith* does not teach a key change command including a new cipher key, the Applicant nonetheless agrees with Examiner Nguyen that the limitation "the first message being indicative of an initiation of a cipher key change" encompasses "a key change command with an operational code" as taught by *Smith*.

Additionally, Examiner Nguyen respectfully asserted in the Final Office Action that a limitation of a specific coding of an acknowledgement (i.e., non data/voice) is not included within any of the claims 9-04. The Applicant respectfully asserts that "the second message being coded with a new cipher key as an acknowledgement of the cipher key change by said terminal" as recited in independent claims 9, 17, 25 and 29 is directed to a specific coding of an acknowledgement.

Finally, Examiner Nguyen respectfully asserted in the Final Office Action that *Smith* teaches a transmission from the controller to the subscriber unit of either a message coded with the new cipher key as an indication that the acknowledgement was deciphered with the new cipher key by the controller or a message coded with the base or old cipher key as an indication of a failure by the controller to decipher the acknowledgment. See, *Smith* at column 3, line 58 to column 4, line 8. However, a careful review of *Smith* reveals that column 3, line 58 to column 4, line 8 of *Smith* is related to the key change command and not the acknowledgment of the key change command.

Pending Claims 9-40. To warrant the anticipation rejection of claims 9-40 by Examiner Nguyen, *Smith* must show each and every limitation of claims 9-40 in as complete detail as in contained in claims 9-40. See, MPEP §2131. As set forth above, the Applicant respectfully traverses this anticipation rejection of claims 9-40, because *Smith* fails to disclose and/or teaches away from the following limitations:

1. "wherein said terminal is operable to transmit a second message to said radio network controller subsequent to a reception of the first message by said terminal, the second message being coded with a new cipher key as an acknowledgement of the cipher key change by said terminal" as recited in independent claim 9;

2. "wherein the first message includes the new cipher key" as recited in dependent claims 10 and 18;

3. "wherein said radio network controller is operable to transmit a third message to said terminal subsequent to a reception of the second message by said radio network controller, the third message being indicative of a deciphering by said radio network controller of the second message with the new cipher key" as recited in dependent claim 11;

4. "wherein the third message is coded with the new cipher key as an indication that said radio network controller deciphered the second message with the new cipher key" as recited in dependent claims 12 and 20;

5. " wherein said radio network controller is operable to transmit a third message to said terminal subsequent to a reception of the second message by said radio network controller, the third message being indicative of a failure by said radio network controller to decipher the second message with the new cipher key" as recited in dependent claim 15;

6. "wherein the third message is coded with an old cipher key as an indication that said radio network controller failed to decipher the second message with the new cipher key" as recited in dependent claims 16 and 24;

7. "means for receiving a second message from the terminal subsequent to a reception of the first message by the terminal, the second message being coded with a new cipher key as an acknowledgement of the cipher key change by the terminal" as recited in independent claim 17;

8. "wherein said radio network controller further includes means for transmitting a third message to the terminal subsequent to a reception of the second message by said radio network controller, the third message being indicative of a deciphering by said radio network controller of the second message with the new cipher key" as recited in dependent claim 19;

9. "wherein said radio network controller further includes means for transmitting a third message to the terminal subsequent to a reception of the second message by said radio network controller, the third message being indicative of a failure by said radio network controller to decipher the second message with the new cipher key" as recited in dependent claim 23;

10. "means for transmitting a second message to the radio network controller subsequent to a reception of the first message by the terminal, the second message being coded with a new cipher key as an acknowledgement of the cipher key change by the terminal" as recited in independent claim 25;

11. "wherein said terminal further includes means for receiving a third message from the radio network controller subsequent to a reception of the second message by the radio network controller, the third message being indicative of a deciphering by the radio network controller of the second message with the new cipher key" as recited in dependent claim 26; and

12. "wherein said terminal further includes means for receiving a third message from the radio network controller subsequent to a reception of the second message by the radio network controller, the third message being indicative of a failure by the radio network controller to decipher the second message with the new cipher key" as recited in dependent claim 28.

13. "the terminal transmitting a second message to the radio network controller subsequent to a reception of the first message by the terminal from the radio network controller, the second message being coded with one of the old cipher key or the new cipher key as an acknowledgement of the cipher key change by the terminal" as recited in independent claim 29;

14. "the radio network controller transmitting a third message to the terminal subsequent to a reception of the second message by the radio network controller from the terminal, the third message being coded with one of the old cipher key or the new cipher key as an indication of one of a successful termination or an unsuccessful termination of the cipher key change" as recited in dependent claim 30;

15. "the radio network controller and the terminal validating the new cipher key" as recited in dependent claim 31;

16. "the radio network controller and the terminal synchronizing a conversion of the old cipher key to the new cipher key" as required in dependent claim 32;

17. "means for receiving a second message from the terminal subsequent to a reception of the first message by the terminal from the radio network controller, the second message being coded with one of the old cipher key or the new cipher key as an acknowledgement of the cipher key change by the terminal" as required in independent claim 33;

18. "means for transmitting a third message to the terminal subsequent to a reception of the second message by the radio network controller from the terminal, the third message being coded with one of the old cipher key or the new cipher key as an indication of one of a successful termination or an unsuccessful termination of the cipher key change" as required in dependent claim 34;

19. "means for validating the new cipher key" as required in dependent claims 35 and 39;

20. "means for synchronizing a conversion of the old cipher key to the new cipher key" as required in dependent claims 36 and 40;

21. "means for transmitting a second message to the radio network controller subsequent to a reception of the first message by the terminal from the radio network controller, the second message being coded with one of the old cipher key or the new cipher key as an acknowledgement of the cipher key change by the terminal" as required in independent claim 37; and

22. "means for receiving a third message from the radio network controller subsequent to a reception of the second message by the radio network controller from the terminal, the third message being coded with one of the old cipher key or the new cipher key as an indication of one of a successful termination or an unsuccessful termination of the cipher key change" as required in dependent claim 38.

Withdrawal of the rejection of pending claims 9-40 under §102(b) as being anticipated by *Smith* is therefore respectfully requested.

SUMMARY

Examiner Nguyen's anticipation rejection of pending claims 9-40 has been obviated by remarking herein supporting an allowance of claims 9-40 over *Smith*. The Applicant respectfully submits that claims 9-40 as listed herein fully satisfy the requirements of 35 U.S.C. §§ 102, 103 and 112. In view of the foregoing, favorable consideration and early passage to issue of the present application is respectfully requested. If any points remain in issue that may best be resolved through a personal or telephonic interview, Examiner Nguyen is respectfully requested to contact the undersigned at the telephone number listed below.

Dated: **January 4, 2005**

Respectfully submitted,
Christoph Hermann

PHILIPS INTELLECTUAL PROPERTY
& STANDARDS
P.O. Box 3001
Briarcliff, New York 10510
Phone: (914) 333-9612
Fax: (914) 332-0615

Jack D. Slobod
Registration No. 26,236
Attorney for Applicant

CARDINAL LAW GROUP
Suite 2000
1603 Orrington Avenue
Evanston, Illinois 60201
Phone: (847) 905-7111
Fax: (847) 905-7113

Frank C. Nicholas
Registration No. 33,983
Attorney for Applicant